IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

US FOODS, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Civil Action No. 1:13-cv-03640
	)	
MICHAEL J. NOBLE, et al.,	)	
	)	
Defendants.	)	
	)	

DECLARATION OF GREGORY CAOUETTE

I, Gregory Caouette, do hereby declare and swear as follows:

1. I am over the age of eighteen (18) and am otherwise competent to give this Declaration. The information contained in this Declaration is based on my personal knowledge.

2. I submit this declaration in support of Plaintiff's Motion for Expedited Discovery in the above-captioned matter.

3. I am a Director of Computer Forensic Operations at Kroll Advisory Solutions ("Kroll"). I have been employed by Kroll since October 2004. In this position, I use numerous computer applications and tools, many of them proprietary to Kroll, to conduct forensic analyses of computers and electronic devices, including retrieving electronic data that has been lost or deleted from a computer or device. Attached hereto as Exhibit A is a true and correct copy of my curriculum vitae.

4. In addition, I am an EnCase Certified Examiner. The EnCase Certified Examiner ("EnCE") program certifies both public and private sector professionals in the use of Guidance Software EnCase computer forensic software. EnCE certification acknowledges that a professional has mastered computer investigation methodology and the use of EnCase software for

EXHIBIT 3

complex computer examinations. Recognized by both the law enforcement and corporate communities as a symbol of in-depth computer forensics knowledge, EnCE certification establishes that an investigator is a skilled computer examiner. I also have received specialized training in computer forensics from "SEARCH" - The National Consortium for Justice Information and Statistics. In addition, I have received further instruction in computer forensics from the National White Collar Crime Center, Guidance Software, Inc., AccessData Corporation, Kroll Ontrack, and other entities through the High Technology Crime Investigation Association.

5. I have previously conducted more than two hundred computer forensic examinations. In addition, I have provided testimony as a computer forensics expert in numerous cases.

6. In late 2012, Kroll was retained by counsel for US Foods to perform a computer forensic examination of the hard drive of a computer issued by US Foods to Phillip G. Roszak ("Roszak"), a former employee.

7. When Kroll is engaged for matters involving electronic evidence, such as here, a computer forensic protocol is used when handling electronic information that may be the subject of litigation. A typical first step of such a protocol is to create a full forensic image of the computer, drive or device. That image is created on a separate piece of sanitized media, as was done in this case.

8. A forensic image is made in order to preserve the integrity of the original data. The imaging process creates an exact duplicate of all data resident on the original computer, drive or device. The imaging process does not change or alter the information on the original computer, drive or device media in any way. The image includes all active data as well as all areas of the computer, drive or device where deleted or partially overwritten files may exist.

9. During the creation of the forensic copy of a hard drive, a Message Digest 5 ("MD5") hash value is generated. The MD5 hash value is a 128-bit (32 character) alphanumeric value that uniquely identifies the contents of a file, drive, or other form of data. The algorithm used to compute the MD5 hash is publicly available and is commonly used in the field of computer forensics to compare two data sets to determine whether they are exactly the same. The likelihood that two different and random data sets have the same hash value is said to be almost "computationally infeasible." In other words, when using the MD5 hash algorithm to compare the identical nature (or lack thereof) of two data sets, the accuracy is said to be far greater than the accuracy of fingerprints or even DNA. Kroll uses the MD5 hash algorithm to validate that the bit-by-bit image is the same as the original data. Kroll used the MD5 hash algorithm on the hard drive previously used by Roszak and validated that the image was the same as the original hard drive.

10. Our examination of the image of Roszak's computer revealed that the user of the computer installed the data destruction utility "CCleaner" on November 23, 2012. CCleaner is a utility that allows a user to delete his activity on a computer, including selecting or targeting for permanent deletion a variety of files, including deleted files in the recycle bin, Internet history files (which shows the internet sites access by the user), cookies, log files, temporary files (which could show a history of documents opened and accessed), registry (which shows the USB and other devices attached to the computer), and program installation files.

11. According to CCleaner's website, the utility is a "system optimization, privacy and cleaning tool. It removes unused files from your system -- allowing Windows to run faster and freeing up valuable hard disk space. ***It also cleans traces of your online activities such as your Internet history. Additionally it contains a fully featured registry cleaner.***" http://www.piriform.com/ccleaner/features.

12. CCleaner also has a feature that allows for the secure deletion of the above-mentioned file types, as well as the ability to delete individual files and folders in a targeted manner.

13. Our examination of Roszak's computer revealed that a significant number of files were deleted prior to Kroll's forensic examination using the tool CCleaner. The user of the computer most recently ran CCleaner on December 11, 2012 starting at 7:25 p.m. Mountain Standard Time ("MST"). When set to delete targeted files securely, the version of CCleaner installed on Roszak's computer will overwrite all data in the file targeted for deletion, including changing the file name to a pattern of 'ZZZ'. Based upon the number of files on the computer that have the 'ZZZ' file name pattern, almost 20,000 files were permanently deleted using the tool CCleaner on December 11, 2012. Although it is impossible to determine the types of files deleted using CCleaner, the deleted files could have included data files, such as Word documents, emails, attachments to emails, pictures, and spreadsheets.

14. Our examination also revealed that the user used Roszak's computer to access Dropbox. Dropbox is a file hosting service that offers cloud storage, file synchronization, and client software. The Dropbox service can be used to access files saved in Dropbox on users' smartphones, tablets and other computers. Roszak could have used Dropbox to upload documents and data from his US Foods-assigned computer to a Dropbox account. The

documents and data that he uploaded to his Dropbox account would then be (and continue to be) accessible to him through any other computer or device.

15. Our examination also revealed that the user attached devices to Roszak's computer that are capable of transferring files and data from the computer to an external device. For example, on December 5, 2012, an iPad 2, which has file transfer and storage capabilities, was attached to Roszak's computer.

I hereby declare under the penalty of perjury under the laws of the United States of America (and pursuant to 28 U.S.C. § 1746) that the foregoing is true and correct. This declaration is executed this 3rd day of June, 2013 in Fountain Valley, California.

Gregory Caouette

CURRICULUM VITAE

Gregory Caouette
Kroll Advisory Solutions
18350 Mt. Langley Street
Suite 110
Fountain Valley, CA 92708
gcaouette@kroll.com

Employment

Kroll Ontrack/Kroll/Kroll Advisory Solutions, Fountain Valley, Los Angeles and San Francisco, California
Senior Technology Specialist/ Computer Forensics Specialist/Consultant/Director, October 2004 – Present

- Manage the Kroll West Coast computer forensics and cyber investigations laboratory.
- Manage the Kroll West Coast technology consulting group.
- Responsible for providing technology consulting in support of the Kroll Business Intelligence and Investigations group.
- Responsible for conducting sound computer forensic analysis and maintaining strict media chain of custody using protocols and procedures in line with generally accepted computer forensics techniques and best practices.
- Acquire and preserve computer media in either a lab setting or through onsite data capture or seizure. This involves creating sector-by-sector forensic copies of original media for legal and investigative purposes.
- Perform data recovery, including both file and e-mail recovery, on electronic media to be analyzed during the course of an engagement.
- Interact with project management to provide the highest quality of service. This includes interaction with attorneys, clients, managers, case managers, legal consultants and Kroll managing directors.
- Conduct analysis of electronic media. Example analysis includes, but is not limited to:
  - Searches for evidence of financial fraud and theft of trade secrets on computer media from desktops, laptops and server platforms, including unauthorized access to computer systems.
  - Searches for evidence of reformatting, dates of reformatting and utilities used to wipe or copy data from electronic media.
  - Locating evidence of improper removal, duplication, destruction or transmission of e-mail messages or files.
- Provide expert testimony and investigative support as needed on various projects.

US Postal Inspection Service, Dallas, Texas
Postal Inspector/Program Manager, 1999 - October 2004

- Managed the digital evidence program for the US Postal Inspection Service in a twelve state region.
- Supervised fifteen full/part time forensic computer analysts in four field divisions and managed the forensic lab in Dallas, Texas.
- Trained personnel in the proper methods of collecting, preserving and processing digital evidence.
- Oversaw and coordinated field search and seizure of computer related evidence.
- Set work priorities and managed work assignments to accomplish desired objectives and goals.
- Conducted over 175 computer forensic examinations.
- Developed Internet Crimes Investigation training course.
- Coordinated numerous multi-agency computer forensic investigations.

EXHIBIT A

US Postal Inspection Service, Memphis, Tennessee
Postal Inspector/Team Leader, 1993 - 1999

- Managed a team of six postal inspectors conducting
  - Fraud investigations
  - Narcotics investigations
  - Adult and child pornography investigations
  - Identity theft investigations
  - Bomb investigations

US Postal Inspection Service, Washington, DC
Postal Inspector/Program Manager, 1992 - 1993

- Information Technology Division.

US Postal Inspection Service, Washington, DC
Postal Inspector/Projects Coordinator, 1989 - 1992

- Internal Affairs Division.

US Postal Inspection Service, Los Angeles, California
Postal Inspector, 1987 – 1989

- Fraud investigations.

US Postal Inspection Service, Shreveport, Louisiana
Postal Inspector, 1984 - 1987

- Miscellaneous Investigations
  - Crimes against the employees and property of the United States Postal Service.
  - Identity theft.
  - Narcotics.
  - Child pornography.

Education

Jones College, Orlando, Florida
B.S., Accounting, Cum Laude, 1981

Experience with Computer Forensics Examinations/Procedures

Approximate number of computer forensic/cyber investigations

- Over 150

Approximate number of pieces of media imaged

- Over 2000

Approximate number of pieces of media examined for potential evidence

- Over 500

Continuing Education

Computer Forensic Investigations – Windows In-Depth, SANS Institute, 36 hours (New Orleans, LA – January 16, 2013 – January 23, 2013)

EnCase® Advanced Computer Forensics, Guidance Software, 32 hours (Pasadena, California - March 2-5, 2010)

Computer Forensics Summit, Kroll Ontrack Inc., 20 hours (November 12-15, 2008)

Apple Certified Macintosh Technician Training, V2 Consulting, 56 hours (San Francisco, California - , March 10-18, 2008)

Computer Forensics Summit, Kroll Ontrack Inc., 20 hours (October 11-12, 2007)

International Training Conference, High Technology Crime Investigation Association (HTCIA), 32 hours (San Diego, California - September 2007)

Ethical Hacking: Security Testing for Professionals, InfoSec Institute, 40 hours (Las Vegas, Nevada - February 26 through March 2, 2007)

Kroll Ontrack Inc., On-the-job training in Kroll Ontrack data recovery technology (2004 - Present)

Computer Forensics Summit, Kroll Ontrack Inc., 20 hours (June 9-10, 2006)

Computer Forensics Summit, Kroll Ontrack Inc., 8 hours (April 2, 2005)

AccessData FTK Advanced Forensic Bootcamp, 25 hours (Eden Prairie, Minnesota - March 30 – April 1, 2005)

International Training Conference, HTCIA, 32 hours (Monterey, California - September 2005)

AccessData FTK Forensic Bootcamp, 40 hours (Houston, Texas - September 2004)

International Training Conference, HTCIA, 32 hours (Lake Tahoe, California - September 2003)

Advanced Data Recovery and Analysis, Microsoft Windows 9x - ME Systems, National White Collar Crime Center, 40 hours (Dallas, Texas - 2003)

EnCase® Trainer Course, EnCase® Intermediate Analysis and Reporting, Guidance Software, 40 hours, Sterling, Virginia, 2003

Forensic Computer Examiner Training Program, IACIS, 80 hours (Orlando, Florida - 2003)

Advanced Data Recovery and Analysis, Internet forensic investigations, National White Collar Crime Center, 40 hours (Dallas, Texas - 2002)

International Training Conference, Miscellaneous forensic topics, HTCIA, 32 hours (Long Beach, California - 2001)

Basic Computer Forensic Training, Forensic Tool Kit, Access Data, 40 hours (Dallas, Texas - 2001)

EnCase® Advanced Training, EnCase Advanced Computer Forensics, Guidance Software, 40 hours (Pasadena, California - 2001)

Advanced Data Recovery and Analysis, Microsoft Windows NT, National White Collar Crime Center, 40 hours (Fairmont, West Virginia - 2001)

SEARCH, The Investigation of Computer Crime, The National Consortium for Justice Information and Statistics, 40 hours (San Francisco, California - 1998)

Apple Certified Macintosh Technician, Apple Computers (ACMT)

Agency Trainer, EnCase® Forensic Software

Certifications

Certified Examiner, Guidance Software, EnCase® (EnCE)

Certified Fraud Examiner, Association of Certified Fraud Examiners (CFE)

Testimony/Court Experience

Angelica Textile Services, Inc v. Jaye Park, Emerald Textiles, LLC., San Diego, California. 2012. Evidentiary Hearing

Angelica Textile Services, Inc v. Jaye Park, Emerald Textiles, LLC., San Diego, California. 2012. Deposition

XP Power LLC v. James Meduri and Does 1-10, Santa Clara, California. 2011. Deposition

Aletheia Research and Management, Inc. v. Joseph M. Boskovich, et al., Los Angeles, California. 2010. Deposition

Bouquet v. Thomson Legal & Regulatory Applications, Inc., Los Angeles, California. 2008. Trial.

Bouquet v. Thomson Legal & Regulatory Applications, Inc., Irvine, California. 2008. Deposition

Latiolais v. Merck, et al., Los Angeles, California. 2007. Deposition.

Shari Nolan v. Merrill Lynch and Phillip Horner, San Francisco, California. 2006. Arbitration Hearing.

Mussell v. Mussell , Minneapolis, Minnesota. 2006.Trial.

United States v. James Naiden, Minneapolis, Minnesota. 2004. Trial.

United States v. Charles Osamor, Houston, Texas. 2003. Trial

United States v. Anthony Venson, Lafayette, Louisiana. 2002.Trial.

Technical/Professional Presentations

Computer Forensics Certification Class, Instructor, California State University - Fullerton, California, March 10, 2005

American Association of Surgical Physicians Assistants (AASPA) Conference, Presenter, "Medical/Legal Risks Posed by the Intersection of Electronic Data, Social Media, Privacy Rules and E-Discovery" – San Francisco, California, October 22, 2011

Professional Organizations

Member, Association of Certified Fraud Examiners (ACFE), 2011 - Present

Member, High Technology Crime Investigation Association (HTCIA), 1999 - Present

Member, International Association of Computer Investigative Specialists (IACIS), 1999 - 2004